

Introduction

This document provides information about the IOS XE software release for the Cisco NCS 4206 and Cisco NCS 4216 beginning with Cisco IOS XE Release 3.18SP.

- Overview of Cisco NCS 4206 and NCS 4216, on page 1
- Feature Navigator, on page 2
- Hardware Supported, on page 2
- Restrictions and Limitations, on page 4
- Determining the Software Version, on page 7
- Upgrading to a New Software Release, on page 7
- Supported FPGA Versions for NCS 4206 and NCS 4216, on page 8
- Additional References, on page 13

Overview of Cisco NCS 4206 and NCS 4216

Cisco NCS 4206

The Cisco NCS 4206 is a fully-featured aggregation platform designed for the cost-effective delivery of converged mobile and business services. With shallow depth, low power consumption, and an extended temperature range, this compact 3-rack-unit (RU) chassis provides high service scale, full redundancy, and flexible hardware configuration.

The Cisco NCS 4206 expands the Cisco service provider product portfolio by providing a rich and scalable feature set of Layer 2 VPN (L2VPN) and Layer 3 VPN (L3VPN) services in a compact package. It also supports a variety of software features, including Carrier Ethernet features, Timing over Packet, and pseudowire.

For more information on the Cisco NCS 4206 Chassis, see the Cisco NCS 4206 Hardware Installation Guide.

Cisco NCS 4216

The Cisco NCS 4216 is a seven-rack (7RU) unit chassis that belongs to the Cisco NCS 4200 family of chassis. This chassis complements Cisco's offerings for IP RAN solutions for the GSM, UMTS, LTE and CDMA. Given it's form-factor, interface types and Gigabit Ethernet density the Cisco NCS 4216 can also be positioned as a Carrier Ethernet aggregation platform.

The Cisco NCS 4216 is a cost optimized, fully redundant, centralized forwarding, extended temperature, and flexible pre-aggregation chassis.

For more information about the Cisco NCS 4216 Chassis, see the Cisco NCS 4216 Hardware Installation Guide.

NCS 4216 14RU

The Cisco NCS 4216 F2B is a 14-rack unit router that belongs to the Cisco NCS 4200 family of routers. This router complements Cisco's offerings for IP RAN solutions for the GSM, UMTS, LTE, and CDMA. Given its form-factor, interface types, and Gigabit Ethernet density the Cisco NCS 4216 14RU can also be positioned as a Carrier Ethernet aggregation platform.

The Cisco NCS 4216 14RU is a cost optimized, fully redundant, centralized forwarding, extended temperature, and flexible pre-aggregation router.

For more information about the Cisco NCS 4216 F2B Chassis, see the Cisco NCS 4216 F2B Hardware Installation Guide.

Feature Navigator

You can use Cisco Feature Navigator to find information about feature, platform, and software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on cisco.com is not required.

Hardware Supported

The following sections list the hardware supported for Cisco NCS 4206 and Cisco NCS 4216 chassis.

Cisco NCS 4206 Supported Interface Modules

Supported Interface Modules

Note If the **license feature service-offload enable** command is configured, then the NCS4200-1T8LR-PS IM is not supported in the router for RSP3.

Note There are certain restrictions in using the interface modules on different slots in the chassis. Contact Cisco Sales/Support for the valid combinations.

Note FAN OIR is applicable every time the IM based fan speed profile is switched to NCS4200-1H-PK= and NCS4200-2Q-P interface modules. Even though the IMs remain in the Out-of-Service state, they are still considered as present in the chassis.

Table 1: NCS420X-RSP Supported Interface Modules and Part Numbers

RSP Module	Supported Interface Modules	Part Numbers	Slot
NCS420X-RSP	8-port 10 Gigabit Ethernet Interface Module (8X10GE)	NCS4200-8T-PS	All
	1-port 100 Gigabit Ethernet Interface Module (1X100GE)	NCS4200-1H-PK=	4 and 5
	2-port 40 Gigabit Ethernet QSFP Interface Module (2X40GE)	NCS4200-2Q-P	4 and 5
	8/16-port 1 Gigabit Ethernet (SFP/SFP) + 1-port 10 Gigabit Ethernet (SFP+) / 2-port 1 Gigabit Ethernet (CSFP) Interface Module	NCS4200-1T16G-PS	0,3,4, and 5
	1-port OC-192 Interface module or 8-port Low Rate Interface Module	NCS4200-1T8S-10CS	2,3,4, and 5
	NCS 4200 1-Port OC-192 or 8-Port Low Rate CEM 20G Bandwidth Interface Module	NCS4200-1T8S-20CS	2,3,4, and 5[1]
	48-port T1/E1 CEM Interface Module	NCS4200-48T1E1-CE	All
	48-port T3/E3 CEM Interface Module	NCS4200-48T3E3-CE	All
	2-port 100 Gigabit Ethernet (QSFP) Interface Module (2X100GE)[2]	NCS4200-2H-PQ	4,5
	1-port OC48[3]/ STM-16 or 4-port OC-12/OC-3 / STM-1/STM-4 + 12-port T1/E1 + 4-Port T3/E3 CEM Interface Module	NCS4200-3GMS	2,3,4, and 5

1 These slots are supported on 10G or 20G mode.
2 IM supports only one port of 100G with RSP3 as QSFP28 on Port 0 in both slots 4 and 5.
3 If OC48 is enabled, then the remaining 3 ports are disabled.

Table 2: NCS420X-RSP-128 Supported Interface Modules and Part Numbers

RSP Module	Supported Interface Modules	Part Numbers	Slot
NCS420X-RSP	SFP Combo IM—8-port Gigabit Ethernet (8X1GE) + 1-port 10 Gigabit Ethernet Interface Module (1X10GE)	NCS4200-1T8LR-PS	All
	8-port T1/E1 CEM Interface Module	NCS4200-8E1T1-CE	All
	1-port OC48[4]/ STM-16 or 4-port OC-12/OC-3 / STM-1/STM-4 + 12-port T1/E1 + 4-Port T3/E3 CEM Interface Module	NCS4200-3GMS	2,3,4, and 5

4 If OC48 is enabled, then the remaining 3 ports are disabled.

Cisco NCS 4216 Supported Interface Modules

For information on supported interface modules, see Supported Interface Modules.

Cisco NCS 4216 F2B Supported Interface Modules

For information on supported interface modules, see Supported Interface Modules.

Restrictions and Limitations



Note The error message "PLATFORM-1-NOSPACE: SD bootflash : no space alarm assert" may occur in the following scenarios:

- Any sector of SD Card gets corrupted
- Improper shut down of router
- power outage.

This issue is observed on platforms which use EXT2 file systems.

We recommend performing a reload of the router. As a result, above alarm will not be seen during the next reload due to FSCK(file systems check) execution.

However, If the error persists after a router reload, we recommend to format the bootflash or FSCK manually from IOS.

- Embedded Packet Capture (EPC) is not supported on ASR 900 routers.
- From the Cisco IOS XE 16.6.1 releases, In-Service Software Upgrade (ISSU) is not supported on the router to the latest releases. For more information on the compatible release versions, see ISSU Support Matrix.
- ISSU is not supported between a Cisco IOS XE 3S release and the Cisco IOS XE Bengaluru 17.6.x release.
- The port restriction on 1-port OC-192 or 8-port low rate CEM interface module is on port pair groups. If you have OC48 configured on a port, the possible port pair groups are 0–1, 2–3, 4–5, 6–7. If one of the ports within this port group is configured with OC48 rate, the other port cannot be used.
- RS422 pinout works only on ports 0–7.
- The **ip cef accounting** command is *not* supported on the router.
- Configuration sync does *not* happen on the Standby RSP when the active RSP has Cisco Software Licensing configured, and the standby RSP has Smart Licensing configured on the router. If the active RSP has Smart Licensing configured, the state of the standby RSP is undetermined. The state could be pending or authorized as the sync between the RSP modules is not performed.
- Evaluation mode feature licenses may not be available to use after disabling, and enabling the smart licensing on the RSP2 module. A reload of the router is required.

- Ingress counters are not incremented for packets of the below format on the RSP3 module for the 10-Gigabit Ethernet interfaces, 100-Gigabit Ethernet interfaces, and 40-Gigabit Ethernet interfaces:

  Packet Format

  MAC header---->VLAN header---->Length/Type

  When these packets are received on the RSP3 module, the packets are not dropped, but the counters are not incremented.

- T1 SAToP, T3 SAToP, and CT3 are supported on an UPSR ring only with local connect mode. Cross-connect configuration of T1, T3, and CT3 circuits to UPSR are not supported.
- PTP is not supported when 8-port 10-Gigabit Ethernet interface module is in oversubscribed mode.
- Port channel 61–64 is not supported in the 16.11.1a release. The range of configurable port channel interfaces has been limited to 60.
- Effective with Cisco IOS XE Everest 16.6.1, the VPLS over Port-channel (PoCH) scale is reduced from 48 to 24 for Cisco ASR 903 RSP3 module.

Note The PoCH scale for Cisco ASR 907 routers is 48.

- The frame drops may occur for packets with packet size of less than 100 bytes, when there is a line rate of traffic over all 1G or 10G interfaces available in the system. This restriction is applicable only on RSP2 module, and is not applicable for RSP3 module.
- One Ternary Content-Addressable Memory (TCAM) entry is utilized for Segment Routing Performance Measurement. This is required for the hardware timestamping to function.
- While performing an auto upgrade of ROMMON, only primary partition is upgraded. Use the **upgrade rom-mon filename** command to upgrade the secondary partition of the ROMMON during the auto upgrade. However, the router can be reloaded during the next planned reload to complete the secondary ROMMON upgrade. This is applicable to ASR 903 and ASR 907 routers.
- In the Cisco IOS XE 17.1.1 release, the EVPN EVI type is VLAN-based by default, and while configuring for the EVPN EVI type, it is recommended to configure the EVPN EVI type as VLAN-based, VLAN bundle and VLAN aware model.
- For Cisco IOS XE Gibraltar Release 16.9.5, Cisco IOS XE Gibraltar Release 16.12.3, and Cisco IOS XE Amsterdam 17.1.x, a minimum disk space of 2 MB is required in the boot flash memory file system for a successful ROMMON auto upgrade process. For a disk space lesser than 2 MB, ROMMON auto upgrade fails and the router reboots. This is applicable to Cisco ASR 903 and Cisco ASR 907 routers.
- In the Cisco IOS XE 16.12.1, 17.1.1, and 17.2.1 releases, IPsec is not supported on the Cisco RSP3 module.
- CEM circuit provisioning issues may occur during downgrade from Cisco IOS XE Amsterdam 17.3.1 to any lower versions or during upgrade to Cisco IOS XE Amsterdam 17.3.1 from any lower versions, if the CEM scale values are greater than 10500 APS/UPSR in protected CEM circuits. So, ensure that the CEM scale values are not greater than 10500, during ISSU to or from 17.3.1.
- Some router models are not fully compliant with all IETF guidelines as exemplified by running the pyang tool with the **lint** flag. The errors and warnings that are exhibited by running the pyang tool with the **lint**

flag are currently noncritical as they do not impact the semantic of the models or prevent the models from being used as part of the toolchains. A script has been provided, "check-models.sh", that runs pyang with **lint** validation enabled, but ignoring certain errors. This allows the developer to determine what issues may be present.

As part of model validation for the Cisco IOS XE Amsterdam 17.3.1 release, "LEAFREF_IDENTIFIER_NOT_FOUND" and "STRICT_XPATH_FUNCTIONS" error types are ignored.

- Test Access Port (TAP) is not supported when the iMSG VLAN handoff feature is enabled on the same node.
- Data Communication Channel (DCC) is not supported in the NCS4200-1T8S-20CS interface module for the Cisco IOS XE Cupertino 17.8.1 release.
- In Cisco IOS XE Dublin 17.12.1, for mLDP Partitioned multicast distribution tree (MDT) to work with PIM-Sparse Mode (SM) traffic, configure only a single ingress PE and ensure that the **strict-rpf interface** command is disabled. Configuring multiple PE ingress is not allowed.
- SF and SD alarms are not supported on T1 and T3 ports for the following interface modules:
  - NCS4200-3GMS
  - NCS4200-48T3E3-CE
  - NCS4200-48T1E1-CE
- In RSP2 and RSP3 modules, during In-Service Software Upgrade (ISSU), interface modules undergo FPGA upgrade.

  The following table details the IM Cisco IOS XE versions during ISSU with respect to FPGA upgrade and the impact of traffic flow for these IMs:

Table 3: Impact on IM during ISSU and FPGA Upgrade

IM	IM Version During ISSU	Pre-ISSU FPGA Upgrade	Post-ISSU Impact on IM	FPGA Version post ISSU
Phase 1	Cisco IOS XE 17.3.x or earlier version to Cisco IOS XE 17.4.x	FPGA upgrade completes and IM starts after the reload process. FPGA version (phase -1) - 0.47	Traffic is impacted during upgrade.	0.75
Phases 1 and 2	Version earlier to Cisco IOS XE 17.8.x	FPGA upgrade completes and IM starts after the reload process. • FPGA version (Phase 1)— 0.47 • FPGA version (Phase 2) • NCS4200-8T-PS—69.22 • Combo IM: 69.24	Traffic is impacted during upgrade.	• FPGA version (Phase 1)—0.75 • FPGA version (Phase 2) • NCS4200-8T-PS—69.24 • Combo IM: 69.32

IM	IM Version During ISSU	Pre-ISSU FPGA Upgrade	Post-ISSU Impact on IM	FPGA Version post ISSU
Phase 1	Cisco IOS XE 17.4.1 or later versions to Cisco IOS XE 17.8.1	IM FPGA already upgraded with the latest version and reload is not required.	Traffic is not impacted.	0.75

For more information on the FPGA versions, see Supported FPGA Versions.

Refer the following table for supported IMs:

Table 4: NCS 4200 Supported Ethernet Interface Module

Phase 1 IM	Phase 2 IM	Phase 3 IM
NCS4200-1T8LR	NCS4200-1T8LR-PS	NCS4200-8T-PS
		NCS4200-2Q-P
		NCS4200-2H-PQ

Determining the Software Version

You can use the following commands to verify your software version:

- Consolidated Package—**show version**
- Individual sub-packages—**show version installed** (lists all installed packages)

Upgrading to a New Software Release

Only the latest consolidated packages can be downloaded from Cisco.com; users who want to run the router using individual subpackages must first download the image from Cisco.com and extract the individual subpackages from the consolidated package.

For information about upgrading to a new software release, see the Upgrading the Software on the Cisco NCS 4200 Series Routers .

Upgrading the FPD Firmware

FPD Firmware packages are bundled with the software package. FPD upgrade is automatically performed ont the router.

If you like to manually change the FPD Firmware software, use the **upgrade hw-module subslot 0/0 fpd bundle** to perform FPD frmware upgrade.

Supported FPGA Versions for NCS 4206 and NCS 4216

Use the **show hw-module all fpd** command to display the IM FPGA version on the chassis.

Use the **show platform software agent iomd** [*slot/subslot*] **firmware cem-fpga** command to display the CEM FPGA version on the chassis.

The table below lists the FPGA version for the software releases.

Note During ISSU, TDM interface modules are reset for FPGA upgrade.

Table 5: Supported TDM IM and CEM FPGAs for NCS 4206-RSP3 and NCS 4216

Category	Cisco IOS XE Release	48 X T1/E1 CEM Interface Module FPGA (NCS 4200-48T1E1-CE)	48 X T3/E3 CEM Interface Module FPGA (NCS 4200-48T3E3-CE)	OC-192 Interface Module + 8-port Low Rate Interface Module FPGA (NCS4 200-1T8S-10CS)	NCS 4200-1T8S-20CS	NCS4200-3GMS
IM FPGA	17.15.6	1.22	1.22	1.15	0.95	2.1
CEM FPGA		70160070	CAS: 72020072 Non-CAS: 56030056	5G mode: 10090065 10G mode: 10070079	20G mode - CAS: 10330075 10G and 20G - Non-CAS: 12290074	CAS: 10930095 Non-CAS: 11060093
CEM FPGA	17.15.5	1.22	1.22	1.15	0.95	2.1
		70160070	CAS: 72020072 Non-CAS: 56030056	5G mode: 10090065 10G mode: 10070079	20G mode - CAS: 10330075 10G and 20G - Non-CAS: 12290074	CAS: 10930095 Non-CAS: 11060093
IM FPGA	17.15.4	1.22	1.22	1.15	0.95	2.1
CEM FPGA		70160070	CAS: 72020072 Non-CAS: 56030056	5G mode: 10090065 10G mode: 10070079	20G mode - CAS: 10330075 10G and 20G - Non-CAS: 12290074	CAS: 10930095 Non-CAS: 11060093

Category	Cisco IOS XE Release	48 X T1/E1 CEM Interface Module FPGA (NCS 4200-48T1E1-CE)	48 X T3/E3 CEM Interface Module FPGA (NCS 4200-48T3E3-CE)	OC-192 Interface Module + 8-port Low Rate Interface Module FPGA (NCS4 200-1T8S-10CS)	NCS 4200-1T8S-20CS	NCS4200-3GMS
IM FPGA	17.15.3b	1.22	1.22	1.15	0.95	2.1
CEM FPGA		70160070	CAS: 72020072 Non-CAS: 56030056	5G mode: 10090065 10G mode: 10070079	20G mode - CAS: 10330075 10G and 20G - Non-CAS: 12290074	CAS: 10930095 Non-CAS: 11060093
IM FPGA	17.15.2	1.22	1.22	1.15	0.95	2.1
CEM FPGA		70160070	CAS: 72020072 Non-CAS: 56030056	5G mode: 10090065 10G mode: 10070079	20G mode - CAS: 10330075 10G and 20G - Non-CAS: 12290074	CAS: 10930095 Non-CAS: 11060093
IM FPGA	17.15.1b	1.22	1.22	1.15	0.95	2.0
CEM FPGA		70160070	CAS: 72020072 Non-CAS: 56030056	5G mode: 10090065 10G mode: 10070079	20G mode - CAS: 10330075 10G and 20G - Non-CAS: 12290074	CAS: 10930095 Non-CAS: 11060093
IM FPGA	17.15.1	1.22	1.22	1.15	0.95	2.0
CEM FPGA		70160070	CAS: 72020072 Non-CAS: 56030056	5G mode: 10090065 10G mode: 10070079	20G mode - CAS: 10330075 10G and 20G - Non-CAS: 12290074	CAS: 10930095 Non-CAS: 11060093
IM FPGA	17.13.1	1.22	1.22	1.15	0.95	2.0
CEM FPGA		70140070	CAS: 72010072 Non-CAS: 56020056	5G mode: 10090065 10G mode: 10070079	20G mode - CAS: 10240075 10G and 20G - Non-CAS: 11160074	CAS: 10810095 Non-CAS: 10950093

Category	Cisco IOS XE Release	48 X T1/E1 CEM Interface Module FPGA (NCS 4200-48T1E1-CE)	48 X T3/E3 CEM Interface Module FPGA (NCS 4200-48T3E3-CE)	OC-192 Interface Module + 8-port Low Rate Interface Module FPGA (NCS4 200-1T8S-10CS)	NCS 4200-1T8S-20CS	NCS4200-3GMS
IM FPGA	17.12.1	1.22	1.22	1.15	0.95	2.0
CEM FPGA		7.0	7.2	5G mode: 6.5 10G mode: 7.9	10G mode: 7.4 20G mode: 7.5	9.5
IM FPGA	17.11.1a	1.22	1.22	1.15	0.95	2.0
CEM FPGA		7.0	5.6	5G mode: 6.5 10G mode: 7.9	10G mode: 7.4 20G mode: 7.5	9.3
IM FPGA	17.10.1	1.22	1.22	1.15	0.95	2.0
CEM FPGA		6.0	5.2	5G mode: 6.5 10G mode: 7.9	10G mode: 7.3 20G mode: 7.3	9.3
IM FPGA	17.9.2	1.22	1.22	1.15	0.95	2.0
CEM FPGA		6.0	5.2	5G mode: 6.5 10G mode: 7.9	10G mode: 7.2 20G mode: 7.2	9.1
IM FPGA	17.9.1	1.22	1.22	1.15	0.93	2.0
CEM FPGA		6.0	5.2	5G mode: 6.5 10G mode: 7.9	10G mode: 7.2 20G mode: 7.2	9.1

Category	Cisco IOS XE Release	48 X T1/E1 CEM Interface Module FPGA (NCS 4200-48T1E1-CE)	48 X T3/E3 CEM Interface Module FPGA (NCS 4200-48T3E3-CE)	OC-192 Interface Module + 8-port Low Rate Interface Module FPGA (NCS4 200-1T8S-10CS)	NCS 4200-1T8S-20CS	NCS4200-3GMS
IM FPGA	17.8.1	1.22	1.22	1.15	0.93	2.0
CEM FPGA		6	5.2	5G mode: 6.5 10G mode: 7.9	10G mode: 7.0 20G mode: 6.0	9.0
IM FPGA	17.7.1	1.22	1.22	1.15	0.93	2.0
CEM FPGA		0x52110052	0x52520052	5G mode: 0x10090065 10G mode: 0x10070079	10G mode: 0x10290051 20G mode: 0x10290051	0x10030076
IM FPGA	17.6.2	1.22	1.22	1.15	0.93	2.0
CEM FPGA		0x52110052	0x52520052	5G mode: 0x10090065 10G mode: 0x10070079	10G mode: 0x10290051 20G mode: 0x10290051	0x10030076
IM FPGA	17.6.1	1.22	1.22	1.15	0.93	2.0
CEM FPGA		0x52110052	0x52520052	5G mode: 0x10090065 10G mode: 0x10070079	10G mode: 0x10290051 20G mode: 0x10290051	0x10030076
IM FPGA	17.5.1	1.22	1.22	1.15	0.93	2.0
CEM FPGA		0x52050052	0x52420052	5G mode: 0x10210063 10G mode: 0x10530078	10G mode: 0x10090051 20G mode: 0x10090051	0x10020076

Table 6: Supported Ethernet IM FPGA/FPD versions for NCS 4206-RSP3 and NCS 4216

Cisco IOS XE Release	NCS4200-1T16G-PS	NCS4200-1T8LR-PS	NCS4200-8T-PS	NCS4200-2Q-P	NCS4200-1H-PK	NCS4200-2H-PQ	NCS4200-1T16LR
17.15.6	1.129	69.32	0.21	0.21	0.20	0.20	69.24
17.15.5	1.129	69.32	0.21	0.21	0.20	0.20	69.24
17.15.4	1.129	69.32	0.21	0.21	0.20	0.20	69.24
17.15.3b	1.129	69.32	0.21	0.21	0.20	0.20	69.24
17.15.2	1.129	69.32	0.21	0.21	0.20	0.20	69.24
17.15.1	1.129	69.32	0.21	0.21	0.20	0.20	69.24
17.15.1b	1.129	69.32	0.21	0.21	0.20	0.20	69.24
17.13.1	1.129	69.32	0.21	0.21	0.20	0.20	69.24
17.12.1	1.129	69.32	0.21	0.21	0.20	0.20	69.24
17.11.1a	1.129	69.32	0.21	0.21	0.20	0.20	69.24
17.10.1	1.129	69.32	0.21	0.21	0.20	0.20	69.24
17.10.1	1.129	69.32	0.21	0.21	0.20	0.20	69.24
17.9.2	1.129	69.32	0.21	0.21	0.22	0.20	69.24
17.9.1	1.129	69.32	0.21	0.21	0.22	0.20	69.24
17.8.1	1.129	69.32	0.21	0.21	0.22	0.20	69.24
17.7.1	1.129	1.129	0.21	0.21	0.22	0.20	69.24
17.6.1	1.129	1.129	0.21	0.21	0.22	0.20	69.24
17.5.1	1.22	1.22	1.15	0.93	2.0	0.23	0.20
17.4.1	1.129	69.24	0.21	0.22	0.20	3.4	1.129

Table 7: FPGA, HoFPGA, and ROMMON Versions for Cisco IOS XE 17.15.1, 17.15.2, 17.15.3b, 17.15.4 , 17.15.5, and 17.15.6 Releases

Platform	Interface Module	FPGA Current Version	FPGA Minimum Required Version	RSP HoFPGA Active	RSP HoFPGA Standby	ROMMON
NCS420X-RSP-128	NCS4200-1T8LR-PS	69.32	69.32	69.32	69.32	15.6(57r)S
NCS4206-RSP	NCS4200-1H-PK	0.20	0.20	69.32	69.32	15.6(57r)S
	NCS4200-8T-PS	0.22	0.21			
	NCS4200-1T8LR-PS	69.32	69.32			

Platform	Interface Module	FPGA Current Version	FPGA Minimum Required Version	RSP HoFPGA Active	RSP HoFPGA Standby	ROMMON
NCS4216-RSP	NCS4200-1H-PK	0.20	0.20	20040034	20040034	15.6(57r)S

Additional References

Deferrals

Cisco IOS software images are subject to deferral. We recommend that you view the deferral notices at the following location to determine whether your software release is affected: http://www.cisco.com/en/US/products/products_security_advisories_listing.html.

Field Notices and Bulletins

- Field Notices—We recommend that you view the field notices for this release to determine whether your software or hardware platforms are affected. You can find field notices at http://www.cisco.com/en/US/support/tsd_products_field_notice_summary.html.
- Bulletins—You can find bulletins at http://www.cisco.com/en/US/products/sw/iosswrel/ps5012/prod_literature.html.

MIB Support

The below table summarizes the supported MIBs on the Cisco NCS 4206 and Cisco NCS 4216.

Supported MIBs		
BGP4-MIB (RFC 1657)	CISCO-IMAGE-LICENSE-MGMT-MIB	MPLS-LDP-STD-MIB (RFC 3815)
CISCO-BGP-POLICY-ACCOUNTING-MIB	CISCO-IMAGE-MIB	MPLS-LSR-STD-MIB (RFC 3813)
CISCO-BGP4-MIB	CISCO-IPMROUTE-MIB	MPLS-TP-MIB
CISCO-BULK-FILE-MIB	CISCO-LICENSE-MGMT-MIB	MSDP-MIB
CISCO-CBP-TARGET-MIB	CISCO-MVPN-MIB	NOTIFICATION-LOG-MIB (RFC 3014)
CISCO-CDP-MIB	CISCO-NETSYNC-MIB	OSPF-MIB (RFC 1850)
CISCO-CEF-MIB	CISCO-OSPF-MIB (draft-ietf-ospf-mib-update-05)	OSPF-TRAP-MIB (RFC 1850)
CISCO-CLASS-BASED-QOS-MIB	CISCO-OSPF-TRAP-MIB (draft-ietf-ospf-mib-update-05)	PIM-MIB (RFC 2934)
CISCO-CONFIG-COPY-MIB	CISCO-PIM-MIB	RFC1213-MIB
CISCO-CONFIG-MAN-MIB	CISCO-PROCESS-MIB	RFC2982-MIB
CISCO-DATA-COLLECTION-MIB	CISCO-PRODUCTS-MIB	RMON-MIB (RFC 1757)
CISCO-EMBEDDED-EVENT-MGR-MIB	CISCO-PTP-MIB	RSVP-MIB

Supported MIBs		
CISCO-ENHANCED-MEMPOOL-MIB	CISCO-RF-MIB	SNMP-COMMUNITY-MIB (RFC 2576)
CISCO-ENTITY-ALARM-MIB	CISCO-RTTMON-MIB	SNMP-FRAMEWORK-MIB (RFC 2571)
CISCO-ENTITY-EXT-MIB	CISCO-SONET-MIB	SNMP-MPD-MIB (RFC 2572)
CISCO-ENTITY-FRU-CONTROL- MIB	CISCO-SYSLOG-MIB	SNMP-NOTIFICATION-MIB (RFC 2573)
CISCO-ENTITY-SENSOR-MIB	DS1-MIB (RFC 2495)	SNMP-PROXY-MIB (RFC 2573)
CISCO-ENTITY-VENDORTYPE-OID-MIB	ENTITY-MIB (RFC 4133)	SNMP-TARGET-MIB (RFC 2573)
CISCO-FLASH-MIB	ENTITY-SENSOR-MIB (RFC 3433)	SNMP-USM-MIB (RFC 2574)
CISCO-FTP-CLIENT-MIB	ENTITY-STATE-MIB	SNMPv2-MIB (RFC 1907)
CISCO-IETF-ISIS-MIB	EVENT-MIB (RFC 2981)	SNMPv2-SMI
CISCO-IETF-PW-ATM-MIB	ETHERLIKE-MIB (RFC 3635)	SNMP-VIEW-BASED-ACM-MIB (RFC 2575)
CISCO-IETF-PW-ENET-MIB	IF-MIB (RFC 2863)	SONET-MIB
CISCO-IETF-PW-MIB	IGMP-STD-MIB (RFC 2933)	TCP-MIB (RFC 4022)
CISCO-IETF-PW-MPLS-MIB	IP-FORWARD-MIB	TUNNEL-MIB (RFC 4087)
CISCO-IETF-PW-TDM-MIB	IP-MIB (RFC 4293)	UDP-MIB (RFC 4113)
CISCO-IF-EXTENSION-MIB	IPMROUTE-STD-MIB (RFC 2932)	CISCO-FRAME-RELAY-MIB
CISCO-IGMP-FILTER-MIB	MPLS-LDP-GENERIC-STD-MIB (RFC 3815)	

MIB Documentation

To locate and download MIBs for selected platforms, Cisco IOS and Cisco IOS XE releases, and feature sets, use Cisco MIB Locator found at the following location: http://tools.cisco.com/ITDIT/MIBS/servlet/index. To access Cisco MIB Locator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to cco-locksmith@cisco.com. An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions found at the following location: http://tools.cisco.com/RPF/register/register.do

Open Source License Notices

For a listing of the license notices for open source software used in Cisco IOS XE 3S Releases, see the documents accessible from the License Information page at the following location:

http://www.cisco.com/en/US/products/ps11174/products_licensing_information_listing.html

.

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.

- To get the business impact you're looking for with the technologies that matter, visit Cisco Services.
- To submit a service request, visit Cisco Support.
- To discover and browse secure, validated enterprise-class apps, products, solutions and services, visit Cisco Marketplace.
- To obtain general networking, training, and certification titles, visit Cisco Press.
- To find warranty information for a specific product or product family, access Cisco Warranty Finder.

Cisco Bug Search Tool

Cisco Bug Search Tool (BST) is a web-based tool that acts as a gateway to the Cisco bug tracking system that maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. BST provides you with detailed defect information about your products and software.